



UNITED STATES PATENT AND TRADEMARK OFFICE

mn

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/473,522	12/28/1999	KENNETH A. PARULSKI	78744PRC	1080
1333 7590 07/25/2007 EASTMAN KODAK COMPANY PATENT LEGAL STAFF 343 STATE STREET ROCHESTER, NY 14650-2201			EXAMINER GYORFI, THOMAS A	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 07/25/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/473,522	Applicant(s) PARULSKI ET AL.	
	Examiner Tom Gyorfi	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 April 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-25 remain for examination.

Response to Arguments

2. In view of the Appeal Brief filed on 4/2/07, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Kim Vu

Supervisory Patent Examiner, Art Unit 2135

Art Unit: 2135

3. Except where noted below, Applicant's arguments with respect to claims 1-25 have been considered but are moot in view of the new ground(s) of rejection.

Regarding the use of the Eastlake reference, Applicant argued on page 11 of the Appeal Brief:

However, at page 14, Eastlake indicates, with emphasis supplied, that even if a separate computer were to receive an input from "a camera with the lens cap on" such data "should not be trusted without some checking in case of hardware failure" and "in any case" will "need to be de-skewed as described elsewhere." This is believed to teach away from the claimed arrangement in which a processor within a digital camera generates a random seed entirely from sensor noise within the digital camera and uses such a random seed to generate a private key and a public key.

Examiner fails to see how this teaches away from the instant invention, for two reasons.

First, the passage quoted by the Applicant is strictly referring to the embodiment where *audio* noise, rather than *image* noise, is used as the source of randomness. Second, allowing for the possibility that de-skewing is required regardless of the source of noise, there is nothing in the claims that forbids de-skewing, or any other form of modification of the random noise as a part of the "generating a random seed" step. To the contrary, the instant specification discloses that the raw image noise generated by the instant invention must be hashed ["de-skewed"] before it is suitable for creating a key pair (page 9, lines 15-20). In any case, it is noted that any camera with a processor capable of compressing images into JPEGs is necessarily capable of performing at least some of the de-skewing techniques disclosed by Eastlake (see sections 5.2.3 and 5.2.4 on page 13 for examples). Nevertheless, this point is academic as the claims of the instant application place no limitations as to exactly how the random seed used to generate the

Art Unit: 2135

public and private keys is itself generated, save that the single input to the algorithm that produces said random seed is the image sensor noise of the camera.

Regarding Applicant's argument that the claims disclose generating the public and private keys inside the camera (e.g. page 6 of the Appeal Brief, 1st paragraph, etc.), it is observed that this argument does not necessarily apply to all of the claims of the instant application. For example, claim 1 recites "a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed the random seed to generate a private key and a public key"; however, the claim language is structured in such a way that, while the processor is located in the digital camera, and the processor performs the recited functions, it does not necessarily follow that the processor has to be inside the camera at the particular moment that it performs the recited functions. Indeed, as observed by the Applicant, the body of prior art previously cited clearly indicates that a processor intended for use in a camera typically generates the keys prior to being installed therein (e.g. Appeal Brief, page 7, 1st paragraph). Claims 9 and 22 also possess similar ambiguities, and are thus similarly flawed; as are all dependent claims therefrom. Should Applicant continue to argue that generating the keys inside the camera is a novel aspect of the instant invention, Examiner suggests that Applicant amend those independent claims in a manner similar to that of claim 6, which unambiguously supports the Applicant's preferred interpretation as currently presented.

Regarding the particular limitations of claim 8 wherein an intermediate step of sending the camera to an authentication service to create the keys used in the camera,

Art Unit: 2135

it is observed that the instant specification teaches that the authorization service can be, in various embodiments, the manufacturer of the camera or alternatively the owner of the camera (page 8, lines 16-19), rendering the additional limitations of this claim as being trivial over the prior art [see below].

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1, 2, and 4-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,889,324 (hereinafter, "Kanai") in view of "RFC 1750: Randomness Recommendations for Security" (hereinafter, "Eastlake").

Regarding claims 1, 6, 9, and 22:

Kanai discloses an improvement to various digital cameras comprising: a processor located within the digital camera for generating a random seed and generating a private key and a public key within the digital camera¹ (col. 7, lines 34-51; col. 8, lines 1-7); and means for storing the private key in a memory of the digital camera for subsequent use of the hash of the digital image to produce the image authentication signature and the metadata signature (col. 4, lines 55-61).

¹ In contrast to the previously cited prior art references, Kanai explicitly discloses wherein the typical arrangement of permanently embedding the private key into the camera at the time of manufacture may be a security risk (col. 1, line 66 – col. 2, line 4); whereas having the camera internally generate the key(s) rectifies the problem (col. 2, lines 50-61).

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures, typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section 5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera – in particular its inclusion of a CPU and RAM – are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term² (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer for the express purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03,

² Webster's II New Riverside University Dictionary defines "computer" as "one that computes, esp. a high-speed electronic device that processes, retrieves, and stores programmed information"; clearly, the cited portions of Kanai indicate that at least the CPU component satisfies that definition.

Art Unit: 2135

see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Regarding claim 7:

Kanai discloses a method of authenticating an image captured by a digital camera, comprising: generating a random seed and generating a private key and a public key in the digital camera (col. 7, lines 34-51; col. 8, lines 1-7); storing the private key in a memory in the digital camera (col. 4, lines 55-61); communicating the public key to a user (Figure 5, step S204); capturing a digital image (col. 5, lines 10-15); hashing the captured digital image in the digital camera to produce an image hash (Figure 2, step S109; col. 6, lines 10-15); encrypting the image hash in the digital camera to produce a digital signature (Figure 2, step S110; col. 6, lines 15-20); and authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside the digital camera (col. 13, lines 1-11).

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures, typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section

Art Unit: 2135

5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera – in particular its inclusion of a CPU and RAM – are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer for the express purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03, see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Regarding claim 8:

Kanai discloses a method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising: manufacturing a digital camera with an internal processor for generating a random seed and generate a private key and a public key within the digital camera (col. 7, lines 34-51; col. 8, lines

Art Unit: 2135

1-7), storing the public key in a memory of the digital camera (col. 4, lines 55-61 and Figure 4), and communicating the public key to a camera operator (Figure 2, steps S204 and S206; col. 7, lines 43-49); sending the digital camera to an authentication service (the manufacturer: col. 7, lines 29-33); activating the digital camera at the authentication service to produce the private key and the public key, and registering the public key at the authentication service (col. 7, lines 29-51); and sending the digital camera to the user (implied by shipping out of the factory: col. 7, lines 29-33).

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures, typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section 5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera, and particularly

Art Unit: 2135

its inclusion of a CPU and RAM, are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer specifically for the purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03, see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Regarding claim 10:

Kanai discloses a method of producing an image authentication signature in a digital camera, comprising: capturing a digital image (col. 5, lines 10-15); compressing the captured digital image (col. 5, lines 15-20); generating a random seed and generate a private key and a public key in the digital camera (col. 7, lines 34-51; col. 8, lines 1-7); storing the private key in a memory in the digital camera (col. 4, lines 55-61); providing one or more metadata values (Figure 2, step S108; col. 6, lines 7-12); hashing the compressed captured digital image and at least one of the metadata values to produce an image hash (Figure 2, step S109; col. 6, lines 10-15); and encrypting the image hash in the digital camera to produce an image authentication signature (Figure 2, step S110; col. 6, lines 15-20);

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures,

typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section 5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera, and particularly its inclusion of a CPU and RAM, are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer specifically for the purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03, see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Art Unit: 2135

Regarding claims 2 and 23:

Kanai further discloses an image sensor for capturing images (Figure 1, element 20; col. 5, lines 5-15); and Eastlake discloses wherein the processor includes means for producing a random seed for the private key by processing an image captured from the image sensor so that the random noise level in the capture image is used in producing the random seed (page 14, section 5.3.1, 1st paragraph).

Regarding claim 4:

Kanai further discloses wherein the processor includes one or more algorithms for producing the random seed (col. 4, lines 45-51; col. 5, lines 30-35) wherein the random seed is used to produce a random number k (Ibid, and col. 8, lines 1-7), and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing (col. 10, lines 20-63).

Regarding claim 5:

Kanai further discloses wherein the processor includes an image processing algorithm using JPEG compression (col. 7, lines 10-12; col. 10, lines 15-20).

Regarding claim 11:

Kanai further discloses the step of storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values (Figure 9; and col. 9, line 44 – col. 10, line 12).

Art Unit: 2135

Regarding claim 12:

Kanai further discloses wherein the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature (col. 6, lines 10-20).

Regarding claim 13:

Kanai further discloses wherein the encrypting step includes encrypting the image hash with a private key to produce the image authentication signature (col. 6, lines 10-20), and further including the step of authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera (col. 13, lines 1-11; cf. col. 12, lines 24-67).

Regarding claim 14:

Kanai further discloses hashing the uncompressed capture digital image to produce a random number k (col. 6, lines 10-20), and wherein the encrypting step uses the random number k to produce the image authentication signature (Ibid).

Regarding claim 15:

Kanai further discloses wherein the encrypting step produces a metadata signature corresponding to the one or more metadata values (col. 12, lines 10-15).

Art Unit: 2135

Regarding claims 16-21:

Kanai further discloses the camera including firmware memory, wherein the private key is produced using an algorithm stored in firmware memory (col. 4, line 35 – col. 5, line 10). Kanai further discloses wherein the encryption and key generation algorithms can at least be updated, suggesting that it is not stored in immutable memory (col. 8, line 8 – col. 9, line 20); furthermore, in certain aspects/embodiments of the Kanai invention, the keys are generated once by the manufacturer prior to being shipped to an end user (col. 7, lines 29-33) and that the public should not be aware of the security algorithms used by the invention (col. 8, line 63 – col. 9, line 3 & lines 15-20). Taking all of these facts into account, it would have been obvious to one of ordinary skill in the art at the time the invention was made to delete the key generating algorithm from the memory of the Kanai camera once the manufacturer had generated the keys. The motivation for doing so would be that such an embodiment would require one less step – authenticating the cipher-processor is obviated – while still maintaining the overall security of the Kanai invention (Kanai: Figure 8, and col. 9, lines 1-8).

Regarding claim 24:

Eastlake further discloses wherein the random noise level is produced by random dark field image data taken from the sensor (as the image sensor is obstructed by another component of the camera: page 14, section 5.3.1, 1st paragraph)

Art Unit: 2135

6. Claims 3 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanai in view of Eastlake as applied to claims 2 and 24 above, and further in view of U.S. Patent 6,046,768 (hereinafter, "Kaneda").

Regarding claims 3 and 25:

Kanai further discloses an analog-to-digital converter coupled to the processor for producing digital signals corresponding to captured images (col. 5, lines 8-15); and Eastlake discloses the processor causing the camera to be in a high gain condition when the initial test image is captured (page 14, section 5.3.1, 1st paragraph). However, neither reference explicitly discloses the use of a variable gain amplifier.

Kaneda discloses a variable gain amplifier coupled to an image sensor for use in a digital camera (Figure 34; col. 17, lines 37-50; col. 27, lines 1-10; col. 28, lines 1-18). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate a variable gain amplifier into the camera disclosed by Kanai, resulting in the ability to amplify the gain as is required by Eastlake. One would be motivated to add a variable gain amplifier to a digital camera because they are also generally useful in correcting image blur from captured images (Kaneda, Ibid).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- U.S. Patent 7,216,232 to Cox et al.
- U.S. Patent 6,968,058 to Kondoh et al.
- U.S. Patent 6,269,446 to Schumacher et al.
- U.S. Patent 5,801,856 to Moghadam et al.
- "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image" by Gary L. Friedman
- "Digital Watermarking for Telltale Tamper Proofing and Authentication" by Deepa Kundur and Dimitrios Hatzinakos
- "The Scientist and Engineer's Guide to Digital Signal Processing" by Steven W. Smith; Chapter 27 discloses wherein the mathematics behind JPEG compression are comparable to at least some of the de-skewing methods taught by Eastlake (Smith, page 3, 2nd and 3rd paragraphs; cf. Eastlake, sections 5.2.3 and 5.2.4)

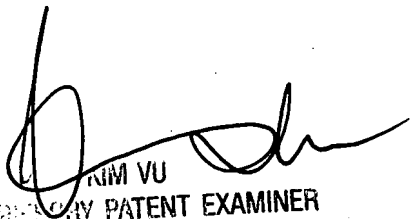
8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
7/16/07


KIM VU
USPTO PATENT EXAMINER
TECHNOLOGY CENTER 2100